



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/443,963	11/19/1999	JAMES PRESCOTT HUGHES	99-064-MIS	8008
7590	01/26/2004		EXAMINER	
WAYNE P BAILEY STORAGE TECHNOLOGY CORPORATION 2270 SOUTH 88TH STREET LOUISVILLE, CO 800280001			MCARDLE, JOSEPH M	
			ART UNIT	PAPER NUMBER
			2132	
			DATE MAILED: 01/26/2004	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/443,963	HUGHES ET AL.
	Examiner Joseph McArdle	Art Unit 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 04 November 2003.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-38 is/are pending in the application.

4a) Of the above claim(s) 2, 4, 17, 19, 23, 25, 34, 36 is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1,3,5-7,9-11,13-16,18,20-22,24,27-29,31-33,35 and 38 is/are rejected.

7) Claim(s) 8,12,26,30 and 37 is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) The proposed drawing correction filed on 04 November 2003 is: a) approved b) disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) The translation of the foreign language provisional application has been received.

15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. The Amendment received on 11/4/2003 has been acknowledged and claims 1, 3, 5-16, 18, 20-22, 24, 26-33, 35, 37 and 38 are pending.

Drawings

2. The informal drawings (Figs. 3A and 3B) filed on 11/04/2003 are acceptable for examination purposes. Applicant is required to submit new formal drawings.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1, 3, 6, 7, 9-11, 13, 14, 16, 18, 21, 22, 24, 27-29, 31-33, 35, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjerrum (5311595) in view of Butler (6094487). In regards to claims 1, 9, 16, 22, 29, and 33 Bjerrum discloses in column 2, lines 49-56 a method of transferring data between computer systems via the use of portable electronic cards. Bjerrum further discloses in column 21, line 31, that the aforementioned electronic cards contain micro processors which meet the limitations set forth under claims 1, 9, 16, 22, 29 and 33 which call for a portable processor. Bjerrum further discloses the use of a production key in column 22, lines 11-

14, which is supplied to the electronic cards and is used to generate keys for use in the encryption and decryption process of the electronic cards as described in column 22 lines 25-32. The production key meets the specified limitations of claims 1, 9, 16, 22, 29, and 33 which call for using a master key. Bjerrum then discloses the use of random numbers in column 23, lines 37-40, which are used by the electronic cards to provide greater security for the generation of keys which are used in the encryption and decryption process. This random number meets the limitations of claims 1, 16, 22, and 33, which calls for the portable processor to use a variable key range variable when generating encryption keys. However, Bjerrum makes no mention of allowing the variable key range variable to be comprised of at least one of a card number, card group number or a reference number representing the number of keys. Butler teaches in column 4, lines 19-30, that smart cards are becoming common place as a result of users desiring a higher degree of identification protection. Butler also discloses in column 4, lines 45-63, that an encryption key can be generated by using shared secret data, which in this case includes the smart card ID (card number). It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Butler's teachings on the uses of smart cards and also how encryption keys can be generated according to a smart card ID (card number) into Bjerrum's design in order to achieve a design that is capable of allowing the variable key range variable to be comprised of at least one of a card number, card group number or a reference number representing the number of keys.

2. In regards to claim 10, Bjerrum further discloses the use of random numbers in column 23, lines 37-40, which are used by the electronic cards to provide greater security for the generation of keys which are used in the encryption and decryption process. This random number meets the limitations set forth under claim 10, which calls for the portable processor to use a variable key range variable when generating encryption keys.
3. In regards to claims 6, 13, 21, 27, 31, and 38 Bjerrum further discloses the use of smart cards in column 21, line 49, which meet the exact limitations set forth by claims 6, 13, 21, 27, 31, and 38.
4. In regards to claims 7, 14, 28, and 32 Bjerrum discloses in column 21, lines 37-38, that the smart cards are validated through the use of a personal identification number, which meets the exact limitations set forth by claims 7, 14, 28, and 32.
5. In regards to claims 3, 11, 18, 24, and 35, Bjerrum discloses in column 24, lines 31-53, a method of verifying encryption and decryption keys used by the portable processors. Bjerrum further discloses that the portable processors will exchange random numbers between each other in order verify each others encryption and decryption keys. The limitations of claims 3, 11, 18, 24, and 35 are met by the above disclose since the random number (which has been shown to represent the variable key range variable from claim 10 above) is outputted from one smart card during an encryption process and received in a second smart card during a decryption process.
6. Claims 5, 15, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjerrum and Butler as applied to claims 1, 10 and 16 above, and further in view of

Dolan (5937068). Bjerrum and Butler's design meets all of the aforementioned limitations of claims 1, 10 and 16 described above. However, Bjerrum and Butler's design lacks the use of a hashing function for generating encryption keys. Dolan shows this exact limitation in column 8, lines 61-62, where it is stated that a smart card generates a hash value and then calculates a key based on that corresponding hash value. It would have been obvious to one of ordinary skill in the art at the time the invention was made to substitute Dolan's teachings into Bjerrum and Butler's design in order to achieve a design that makes use of a hashing function in order to aid in the generation of encryption and decryption keys.

Conclusion

7. Claims 8, 12, 26, 30, and 37 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7239.

Art Unit: 2132

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

jmm
Joseph McArdle
Examiner
Art Unit 2132

jmm

Gilberto 37
GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100